

POWER MAP PERMUTATIONS AND SYMMETRIC DIFFERENCES IN FINITE GROUPS

MÁRTON HABLICSEK AND GUILLERMO MANTILLA-SOLER

ABSTRACT. Let G be a finite group. For all $a \in \mathbb{Z}$, such that $(a, |G|) = 1$, the function $\rho_a : G \rightarrow G$ sending g to g^a defines a permutation of the elements of G . Motivated by a recent generalization of Zolotarev's proof of classic quadratic reciprocity, due to Duke and Hopkins, we study the signature of the permutation ρ_a . By introducing the group of conjugacy equivariant maps and the symmetric difference method on groups, we exhibit an integer d_G such that $\text{sgn}(\rho_a) = \left(\frac{d_G}{a}\right)$ for all G in a large class of groups, containing all finite nilpotent and odd order groups.

1. INTRODUCTION

Given an odd prime p and an integer m not divisible by p , the map $l \mapsto lm$ for integers l defines a permutation ρ_m on $\mathbb{Z}/p\mathbb{Z}$. The map $m \mapsto \rho_m$ can be viewed as a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ into the symmetric group S_p , and composition with the signature homomorphism from S_p to $\{1, -1\}$ yields a homomorphism σ defined on $(\mathbb{Z}/p\mathbb{Z})^*$. Note that for k a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ we have that ρ_k is a $(p-1)$ -cycle, and hence $\sigma(k) = -1$. In particular we have that σ is nontrivial. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of even order there is a unique nontrivial homomorphism from $(\mathbb{Z}/p\mathbb{Z})^*$ into $\{1, -1\}$. It follows that $\sigma(m)$ is equal to $\left(\frac{m}{p}\right)$ where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. Using clever combinatorial arguments, the above characterization of the Legendre symbol, and the Chinese Remainder Theorem, Zolotarev [Z] obtains a group-theoretic proof of quadratic reciprocity. Motivated by Zolotarev's work, Duke and Hopkins define for any finite group G the homomorphism $\left(\frac{\cdot}{G}\right)_{DH} : (\mathbb{Z}/|G|\mathbb{Z})^* \rightarrow \pm 1$ as follows: Let C_1, \dots, C_m be the conjugacy classes of G . Then, for all $a \in \mathbb{Z}$, relatively prime to $|G|$, the map $\psi_a : \{C_1, \dots, C_m\} \rightarrow \{C_1, \dots, C_m\}$ sending C_i to C_i^a is a permutation in S_m . Define $\left(\frac{a}{G}\right)_{DH}$ to be the signature of (ψ_a) . Duke and Hopkins define the *discriminant* D_G of G as follows:

$$D_G = (-1)^s \prod_C \frac{|G|}{|C|},$$

where the product runs over real conjugacy classes C , and s is the number of pairs of nonreal conjugacy classes. Recall that the *Kronecker symbol* is the unique extension of the Legendre symbol to a symbol $\left(\frac{n}{a}\right)$ defined for any $n, a \in \mathbb{Z}$ characterized by the following:

For all integers n, a, b

(i)

$$\left(\frac{n}{a}\right) \left(\frac{n}{b}\right) = \left(\frac{n}{ab}\right),$$

(ii)

$$\left(\frac{n}{2}\right) = \begin{cases} 0 & \text{if } n \equiv 0 \pmod{2} \\ 1 & \text{if } n \equiv 1, 7 \pmod{2} \\ -1 & \text{if } n \equiv 3, 5 \pmod{2}, \end{cases}$$

(iii)

$$\left(\frac{n}{-1}\right) = \begin{cases} 1 & \text{if } n \geq 0 \\ -1 & \text{if } n \leq 0, \end{cases}$$

(iv)

$$\left(\frac{n}{0}\right) = \begin{cases} 0 & \text{if } n \neq 1 \\ 1 & \text{if } n = 1. \end{cases}$$

When a is not odd and positive, some authors (e.g. [D-H]) define $\left(\frac{n}{a}\right)$ only when $n \equiv 0, 1 \pmod{4}$. All the results described here are valid under any of these two conventions, but to be consistent with [D-H] we only use the restricted Kronecker symbol. The main result of [D-H] is the following:

Theorem 1.1 (Duke-Hopkins, 2004). *For all $a \in \mathbb{Z}$ with $(|G|, a) = 1$*

$$\left(\frac{a}{G}\right)_{DH} = \left(\frac{D_G}{a}\right)$$

where D_G is the discriminant of G .

Observe that the discriminant of $G = \mathbb{Z}/p\mathbb{Z}$ is $(-1)^{\frac{p-1}{2}}p$. By applying Theorem 1.1 to $G = \mathbb{Z}/p\mathbb{Z}$, Duke and Hopkins obtain the statement of quadratic reciprocity.

Suppose now that G is a finite group of order n with m conjugacy classes. The homomorphism $\left(\frac{\cdot}{G}\right)_{DH}$ is a generalization of Zolotarev's homomorphism that depends only on the conjugacy classes of G . The work presented in this paper explores the more direct generalization obtained by taking powers of elements. To be more explicit, if we take powers of elements instead of powers of conjugacy classes we obtain a permutation in S_n instead of a permutation in S_m . Let $\left(\frac{\cdot}{G}\right)_{el}$ be the signature of the permutation in elements. Of course, in the case of abelian groups, $\left(\frac{\cdot}{G}\right)_{el}$ and $\left(\frac{\cdot}{G}\right)_{DH}$ are the same, however for nonabelian groups the situation is quite different. Since symmetric groups, dihedral and quaternion groups of order 8 are rational groups (i.e. every two elements of the group generating the same cyclic subgroup are conjugate), it follows that the character $\left(\frac{\cdot}{G}\right)_{DH}$ is trivial for all of them. On the other hand a calculation shows that $\left(\frac{\cdot}{G}\right)_{el}$ is nontrivial for S_3, S_4, D_8 and Q_8 . It is natural to ask if there is a simple characterization of $\left(\frac{\cdot}{G}\right)_{el}$ analogous to the one given by Duke and Hopkins in Theorem 1.1.

For G a finite group, and non-negative integer m , denote the number of Sylow 2-subgroups by $n_2(G)$ and let $f_m(G) = \{g \in G : g^m = 1\}$. Furthermore let $\epsilon(G) = \begin{cases} 1 & \text{if } |G| = 2n_2(G)^1 \\ 0 & \text{otherwise} \end{cases}$.

Definition 1.2. Let G be a finite group. Define

$$d_G := (-1)^{\frac{|G| - |f_2(G)|}{2}} \frac{|G|^{|f_2(G)|}}{n_2(G)^{\epsilon(G)}}.$$

¹These are the groups G of order $2n$ where n is odd and all elements of even order are involutions.

Remark 1.3. Notice that up to square factors the formula for d_G can be rewritten as follows:

- $(-1)^{\frac{|G|-1}{2}}|G|$ if G has odd order,
- $(-1)^{\frac{|G|-|f_2(G)|}{2}}\frac{|G|}{2}$ if $|G| = 2n_2(G)$,
- $(-1)^{\frac{|G|-|f_2(G)|}{2}}$ otherwise.

We opted for the definition for d_G , and not for the above “simplifications”, since it is a closer analog to discriminant D_G defined by Duke and Hopkins. For example, for an abelian or odd order group G we have that D_G and d_G are exactly the same, not only up to square factors. Moreover, as we see next, under this definition the Kronecker symbol $\left(\frac{d_G}{\cdot}\right)$ is always defined (even in the “restricted” sense).

Lemma 1.4. *For any finite group G , we have $d_G \equiv 0$ or $1 \pmod{4}$.*

Proof. Let $n = |G|$. If n is odd, we have that $d_G = (-1)^{\frac{n-1}{2}}n \equiv 1 \pmod{4}$. If n is even, $2^{f_2}|d_G|$ and since $n \equiv |f_2(G)| \pmod{2}$ we have that $d_G \equiv 0 \pmod{4}$ in that case. \square

The following is the main result of this paper.

Theorem 1.5. *Let G be a finite group. Suppose either that G is the direct product of an odd-order group and a 2-group or a group of order $2n$ where n is odd and all elements of even order are involutions.*

Then,

$$\left(\frac{m}{G}\right)_{el} = \left(\frac{d_G}{m}\right)$$

for all m such that $(m, |G|) = 1$.

Remark 1.6. Note that nilpotent and odd order groups satisfy the conditions of the Theorem.

The properties given in Theorem 1.5 are sufficient but not necessary. For example, if G is isomorphic to any group of order 24 the conclusion of Theorem 1.5 also holds. Furthermore, among the 148 groups of order no bigger than 35 there are only four² groups not satisfying the conclusion of Theorem 1.5. We wonder if it is possible to give a complete characterization of groups for which $\left(\frac{m}{G}\right)_{el} = \left(\frac{d_G}{m}\right)$ for all m such that $(m, |G|) = 1$.

By using the method of symmetric differences on groups (see Corollary 4.10) we show that for every group G there exists an integer d_G^* such that

$$\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G^*}{a}\right)$$

for all a satisfying $(a, |G|) = 1$.

Remark 1.7. It would be interesting to see if it is possible to write a “nice exact” formula for d_G^* . We observe that for all groups of order less than 36 we have that $d_G^* = n_2(G)^{v(G)}d_G$ where $v(G)$ is either 0 or 1.

²two groups of order 30, one of order 20 and one of order 18

2. CONJUGACY EQUIVARIANT MAPS

Definition 2.1. Let G be a finite group and let $f : G \rightarrow G$ be an injective map. We say that f is *conjugacy equivariant* if for all $x, g \in G$ we have that $g^{-1}f(x)g = f(g^{-1}xg)$. We denote the set of conjugacy equivariant functions of by $\text{Sym}(G)^G$.

Let $\text{Sym}(G)$ be the group of bijections from G to itself. Notice that $\text{Sym}(G)$ is naturally a G -group under an action for which $\text{Sym}(G)^G$ is just the subgroup of $\text{Sym}(G)$ fixed by G .

Remark 2.2. Note that the function $\Gamma : a \mapsto \rho_a$ is a homomorphism from $(\mathbb{Z}/|G|\mathbb{Z})^*$ to a subgroup of $\text{Sym}(G)^G$. If z is a nontrivial element of the center of G , then the element of $\text{Sym}(G)^G$ defined by multiplication by z is not in the image of Γ .

Let n be the order and m be the number of conjugacy classes of G . Notice that there are natural homomorphisms ψ_C and ρ_{el} from $\text{Sym}(G)^G$ to S_m and S_n respectively. With this observation in mind we define the following quadratic characters³ of $\text{Sym}(G)^G$.

$$\left(\frac{\cdot}{G}\right)_C : \text{Sym}(G)^G \xrightarrow{\psi_C} S_m \xrightarrow{\text{sgn}} S_m/A_m = \{\pm 1\}$$

and

$$\left(\frac{\cdot}{G}\right)_{El} : \text{Sym}(G)^G \xrightarrow{\rho_{el}} S_n \xrightarrow{\text{sgn}} S_n/A_n = \{\pm 1\}.$$

Our next result is a key ingredient in obtaining Theorem 1.5.

Theorem 2.3. *Let G be a finite group of odd order. Then*

$$\left(\frac{\cdot}{G}\right)_C = \left(\frac{\cdot}{G}\right)_{El}.$$

Proof. Let $f \in \text{Sym}(G)^G$ and let $\sigma = (C_1, \dots, C_j)$ be a cycle that appears in the cycle decomposition of $\psi_C(f)$. Let

$$C_\sigma = \bigcup_{i=1}^j C_i.$$

Notice that f restricts to a bijection of the set C_σ and if we denote this restriction by f_σ , then the cycle decomposition of f_σ will be a subset of the cycle decomposition of $\rho_{el}(f)$. It follows that

$$\rho_{el}(f) = \prod_{\sigma} f_\sigma$$

whenever

$$\psi_C(f) = \prod_{\sigma} \sigma.$$

It suffices, therefore, to show that

$$\text{sgn}(f_\sigma) = \text{sgn}(\sigma).$$

Since the classes in the cycle σ all have the same size $|C_1|$, we see that $|C_\sigma| = j|C_1|$. Notice that all the cycles appearing in the cycle decomposition of f_σ have the same length, and that length a must be a multiple of j , say $a = jk$. Then $|C_\sigma| = jkr$, where r is the number of disjoint cycles of f_σ . Since $|C_\sigma| = j|C_1|$ we obtain $kr = |C_1|$, and since $|G|$ is odd we conclude that k and r are odd. In particular,

$$\text{sgn}(f_\sigma) = ((-1)^{jk-1})^r = (-1)^{j-1} = \text{sgn}(\sigma).$$

□

³We abuse the terminology by allowing the trivial homomorphism to be called quadratic.

Corollary 2.4. *Let G be a finite group of odd order. Then the signature of the power map permutation on conjugacy classes agrees with the signature of the power map permutation on elements, or in other words,*

$$\left(\frac{\cdot}{G}\right)_{DH} = \left(\frac{\cdot}{G}\right)_{el}.$$

Proof. Let $a \in (\mathbb{Z}/|G|\mathbb{Z})^*$, and let ρ_a be the bijection on G given by raising to the a^{th} power. Then

$$\left(\frac{a}{G}\right)_{DH} = \left(\frac{\rho_a}{G}\right)_C = \left(\frac{\rho_a}{G}\right)_{El} = \left(\frac{a}{G}\right)_{el}.$$

□

3. ABELIAN GROUPS, ODD ORDER GROUPS AND 2-GROUPS

In this section we prove Theorem 1.5 for abelian groups, groups of odd order, 2-groups, and groups such that the set of elements of odd order form a subgroup of index 2.

Let $n > 1$ be an integer, and let a be an integer relatively prime to n . We denote the multiplicative order of a , as an element of $(\mathbb{Z}/n\mathbb{Z})^*$; by $o_n(a)$. Also for a given group G we denote the total number of elements in G of order n by $G(n)$.

Proposition 3.1. *Let G be a finite group which is either abelian or has odd order. Then, $\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G}{a}\right)$ for all $(a, |G|) = 1$.*

Proof. We have

$$\left(\frac{\cdot}{G}\right)_{el} = \left(\frac{\cdot}{G}\right)_{DH} = \left(\frac{D_G}{\cdot}\right),$$

where the first equality holds by Corollary 2.4 if $|G|$ is odd and it is obvious if G is abelian, and the second equality holds by Theorem 1.1. It suffices, therefore, to show that $D_G = d_G$ if $|G|$ is odd or G is abelian. By the above equalities we have that the sign of D_G is equal to $\left(\frac{-1}{G}\right)_{el}$. Now, raising to the power -1 is a permutation of G that can be written as a product of $(|G| - |f_2(G)|)/2$ disjoint transpositions, i.e. $\prod_{g \neq f_2(G)} (g, g^{-1})$. Therefore if G has

odd order we have that $(-1)^s = (-1)^{(|G|-1)/2}$. On the other hand, odd order groups are characterized by having a unique real class, so $D_G = (-1)^{(|G|-1)/2}|G|$. Then by definition we have that $d_G = (-1)^{(|G|-1)/2}|G|$ for G an odd order group, hence $D_G = d_G$ for such a G . If G is abelian, then a real conjugacy class consists only of one element in $f_2(G)$. So $D_G = d_G$ in this case as well.

□

Corollary 3.2. *Let G be a finite group of order $2n$ where n is odd and all elements of even order are involutions. Then, $\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G}{a}\right)$ for all $(a, |G|) = 1$.*

Proof. Notice first that $n_2(G) = n$, otherwise any element of order 2 would be properly contained in its centralizer yielding to elements of even order that are not involutions. Let H be a subgroup of G of order n . Since $n_2(G) = n$, we have that $|f_2(G)| = n + 1$. In particular G is the disjoint union of H and $f_2(G) \setminus \{1\}$. Since raising to an odd power fixes $f_2(G)$ elementwise, we have that $\left(\frac{a}{G}\right)_{el} = \left(\frac{a}{H}\right)_{el}$ for all $(a, |G|) = 1$. Then, by Proposition 3.1 we have that $\left(\frac{a}{G}\right)_{el} = \left(\frac{d_H}{a}\right)$ for all $(a, |G|) = 1$. Our result follows since

$$d_G = d_H(n^{(n-1)/2}2^{(n+1)/2})^2.$$

□

Proposition 3.3. *Let G be a finite group and let a be an integer coprime to the order of G . Then*

$$\left(\frac{a}{G}\right)_{el} = \prod_{\substack{d||G| \\ d \neq 1,2}} \left((-1)^{\frac{\phi(d)}{o_d(a)}}\right)^{\frac{G(d)}{\phi(d)}}$$

where ϕ denotes the Euler totient function.

Proof. Let d be a divisor of $|G|$, and let G_d be the set of elements of G of order d . Notice that G_d is invariant under the permutation ρ_a of G defined by raising to the a^{th} power. Since G is the disjoint union of G_d , where d runs over all divisors of $|G|$, we have that

$$\left(\frac{a}{G}\right)_{el} = \prod_{d||G|} \text{sign}(\rho_a \upharpoonright_{G_d}).$$

Moreover, we may assume that $d \neq 1, 2$ since for those cases $\rho_a \upharpoonright_{G_d}$ is the trivial permutation. Let x be an element of order d , and notice that

$$(x, x^a, \dots, x^{a^{o_d(a)}})$$

is the element of the cycle decomposition of $\rho_a \upharpoonright_{G_d}$ that contains x . Since x is an arbitrary element we have that $\rho_a \upharpoonright_{G_d}$ is a product of $\frac{G(d)}{o_d(a)}$ cycles with the same cycle structure as the one containing x . Therefore,

$$\text{sign}(\rho_a \upharpoonright_{G_d}) = \left((-1)^{(o_d(a)-1)\left(\frac{G(d)}{o_d(a)}\right)}\right).$$

Since $\phi(d)|G(d)$ for all positive integer d , and $\phi(d)$ is even for all $d \geq 3$ the result follows. □

Now we will deal with the case when G is a 2-group:

Proposition 3.4. *Let G be a finite 2-group. Then $\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G}{a}\right)$ for all $(a, |G|) = 1$.*

Proof. Suppose that $|G| = 2^n$. By Proposition 3.1 we may assume that $n \geq 3$. Also, as we saw during the proof of Proposition 3.1, the permutation ρ_{-1} can be written as a product of $(|G| - |f_2(G)|)/2$ disjoint transpositions. It follows from the definition of d_G for 2-groups that

$$\left(\frac{-1}{G}\right)_{el} = (-1)^{\frac{|G| - |f_2(G)|}{2}} = \left(\frac{d_G}{-1}\right).$$

In particular, since the Kronecker symbol is multiplicative, it is enough to prove the result whenever a is an odd prime p . Since $f_2(G)$ is even, we must show that

$$\left(\frac{p}{G}\right)_{el} = \left(\frac{-1}{p}\right)^{\frac{|G| - |f_2(G)|}{2}}.$$

First we show that

$$\left(\frac{p}{G}\right)_{el} = \left(\frac{-1}{p}\right)^{\frac{G(4)}{2}}.$$

Let $d = 2^k$ be a divisor of $|G|$, and suppose that $3 \leq k$. Since

$$\left(\mathbb{Z}/2^k\mathbb{Z}\right)^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$$

we have that $\frac{\phi(d)}{o_d(p)}$ is even. Therefore, by Proposition 3.3, we have that

$$\left(\frac{p}{G}\right)_{el} = \left((-1)^{\frac{2}{o_4(p)}}\right)^{\frac{G(4)}{2}} = \left(\frac{-1}{p}\right)^{\frac{G(4)}{2}}.$$

Since 4 divides $|G|$, Frobenius' Theorem (see [I-R]) yields that 4 divides $|f_4(G)|$. Therefore $|G| \equiv |f_4(G)| \pmod{4}$. Furthermore $|f_4(G)| - |f_2(G)| = G(4)$ hence $|G| - |f_2(G)| \equiv G(4) \pmod{4}$ and the statement follows. \square

4. SYMMETRIC DIFFERENCES OF GROUPS

In this section we develop the method of symmetric differences of groups, and apply it to obtain the final step in the proof of Theorem 1.5.

Let Δ be the usual symmetric difference operator in sets (i.e., $X\Delta Y = (X \cup Y) \setminus (X \cap Y)$), and let us denote the order of an element g by $o(g)$.

Next we prove that for every finite group G there exist an integer t , and cyclic subgroups C_1, C_2, \dots, C_t of G such that $G = \Delta_{i=1}^t C_i$. We call such decomposition $\Delta_{i=1}^t C_i$ a *cyclic decomposition*. Furthermore, we say that a cyclic decomposition $\Delta_{i=1}^t C_i$ is *reduced* if $C_i \neq C_j$ whenever $i \neq j$.

Notice that a finite group G admits different cyclic decompositions, however:

Lemma 4.1. *Let G be a finite group. Then G admits a unique reduced cyclic decomposition up to the ordering of the cyclic subgroups.*

Proof. Let us begin with an observation. If x and y are two elements of a group G generating the same cyclic subgroup then for every subgroup H we have $x \in H$ if and only if $y \in H$. Therefore if G_1, \dots, G_l are some subgroups of G then $x \in \Delta_{i=1}^l G_i$ if and only if $y \in \Delta_{i=1}^l G_i$. The main consequence of this observation is the following: let x be a generator for a cyclic subgroup C and let G_1, \dots, G_l be some subgroups, then $x \in \Delta_{i=1}^l G_i$ if and only if any other generator of C will be contained in $\Delta_{i=1}^l G_i$.

Now let us prove first the existence. Enumerate the cyclic subgroups of G decreasingly with respect to their order. In other words, write the cyclic subgroups of G as $C_1, C_2, \dots, C_k = 1$ where $|C_i| \geq |C_j|$ whenever $i \leq j$. Also let us choose one generator for every cyclic subgroup, so we have k elements of G : g_1, \dots, g_k . From the enumeration we can see that $o(g_i) \geq o(g_j)$ whenever $i \leq j$.

Now construct subsets $U_i \subseteq G$ recursively, as follows: Set $U_1 = C_1$ and for $i > 1$, let

$$U_i = \begin{cases} U_{i-1} \Delta C_i & \text{if } g_i \notin U_{i-1} \\ U_{i-1} & \text{otherwise} \end{cases}$$

We must show that $U_k = G$, so we prove that every element g of G is contained in U_k . Let $g \in G$, and let C_i be the group generated by g . By the above observation we only have to check that $g_i \in U_k$. Clearly, $g_i \in U_i$, so if we suppose that $g_i \notin U_k$, there is some smallest subscript $j > i$ such that $g_i \notin U_j$. Then $g_i \in U_{j-1}$, so $U_{j-1} \neq U_j$, and thus $U_j = U_{j-1} \Delta C_j$. Therefore $g_i \in C_j$, but since g_i is a generator for C_i , hence $C_i \subset C_j$. Thus $|C_i| < |C_j|$, which contradicts the ordering of the cyclic subgroups.

Now we prove the uniqueness. Suppose \mathcal{B} and \mathcal{C} are collections of distinct cyclic subgroups of G such that $\Delta\mathcal{B} = G = \Delta\mathcal{C}$. If $\mathcal{B} \neq \mathcal{C}$ then choose a cyclic subgroup B of largest possible order such that B is contained in exactly one of the two collections. We can assume that $B \in \mathcal{B}$. Let $B = \langle b \rangle$. Now let us consider cyclic subgroups of G other than B containing b . Every such subgroup is strictly larger than B , and hence it lies either in both of the collections or neither. Since $b \in B$, it follows that b is contained in exactly one more member of \mathcal{B} than \mathcal{C} . This is a contradiction, since b lies in an odd number of members of \mathcal{B} and an odd number of members of \mathcal{C} . \square

It is slightly more convenient to work with elements instead of the subgroups generated by them, therefore instead of writing $G = \Delta_{i \in I} C_i$ from now on we will write $G = \Delta_{i=1}^t \langle g_i \rangle$. With this notation:

Example 4.2. $Q = \langle i \rangle \Delta \langle j \rangle \Delta \langle k \rangle$, where Q denotes the quaternion group with the usual notations.

Example 4.3. $S_3 = \langle (123) \rangle \Delta \langle (12)(3) \rangle \Delta \langle (13)(2) \rangle \Delta \langle (1)(23) \rangle \Delta \langle (1)(2)(3) \rangle$.

We can make the following observations:

Lemma 4.4. *Let G be an arbitrary finite group and let us express G as a symmetric difference of some cyclic subgroups, i.e. $G = \Delta_{i=1}^t \langle g_i \rangle$. Then:*

- (i) t is odd,
- (ii) *If G is a nontrivial 2-group and the decomposition is the reduced cyclic decomposition then none of the g_i is equal to the identity.*

Proof. (i) follows immediately since $1 \in \langle g_i \rangle$ for all i . To show (ii), notice that every non-trivial cyclic subgroup of a nontrivial finite 2-group G has exactly one involution. Furthermore, if $G = \Delta_{i=1}^t \langle g_i \rangle$, then each involution lies in an odd number of members of $\langle g_i \rangle$. Since the number of involutions in G is odd, hence in the decomposition we need odd number of nontrivial cyclic subgroup. Furthermore, by part (i) we know that t is odd thus the statement follows. \square

Furthermore, symmetric differences work nicely with direct products:

Lemma 4.5. *Assume that $G = H \times K$ where the orders of H and K are coprime. Let $H = \Delta_{i=1}^h \langle h_i \rangle$ and $K = \Delta_{j=1}^k \langle k_j \rangle$. Then $G = \Delta_{i=1 \dots h, j=1 \dots k} \langle (h_i, k_j) \rangle$.*

Proof. Since the order of H and the order of K are coprime we see that (h, k) is in $\langle (h_i, k_j) \rangle$ if and only if $h \in \langle h_i \rangle$ and $k \in \langle k_j \rangle$. We know that both $h \in \langle h_i \rangle$ and $k \in \langle k_j \rangle$ hold for odd number of indices therefore $(h, k) \in \langle (h_i, k_j) \rangle$ holds an odd number of times. It follows that $G = \Delta_{i=1 \dots h, j=1 \dots k} \langle (h_i, k_j) \rangle$. \square

We now apply symmetric differences for the remaining cases of Theorem 1.5. We will restrict the power map permutation to the cyclic subgroups in the decomposition above.

Definition 4.6. X is a power-invariant set in G if for every $x \in X$ and for every a which is relatively prime to the order of G , we have $x^a \in X$.

For example, any subgroup is a power-invariant subset. Furthermore:

Lemma 4.7. *If X and Y are power-invariant sets in a finite group G , then, $X^c = G \setminus X$, $X \cap Y$, $X \cup Y$, $X \setminus Y$ and $X \Delta Y$ are power-invariant sets.*

Proof. The first three statements are immediate. The fourth follows from $X \setminus Y = X \cap Y^c$. Finally, the fifth comes from the third and fourth. \square

Let G be a finite group with a power-invariant subset X . If $a \in \mathbb{Z}$ is relatively prime to $|G|$, denote the sign of the permutation induced by a on X by $\left(\frac{a}{X}\right)_{el}$.

Lemma 4.8. *If X and Y are two power-invariant sets, then:*

$$\left(\frac{a}{X\Delta Y}\right)_{el} = \left(\frac{a}{X}\right)_{el} \left(\frac{a}{Y}\right)_{el}.$$

Proof. First we can see that if X and Y are disjoint power-invariant sets then $X\Delta Y = X \cup Y$. In this case a decomposition of $X \cup Y$ as a union of permutation cycles gives us a decomposition of X and of Y as a union of permutation cycles therefore $\left(\frac{a}{X\Delta Y}\right)_{el} = \left(\frac{a}{X \cup Y}\right)_{el} = \left(\frac{a}{X}\right)_{el} \left(\frac{a}{Y}\right)_{el}$.

In the general case by definition we know that $X\Delta Y = (X \setminus Y) \cup (Y \setminus X)$ furthermore the latter two sets are disjoint thus:

$$\left(\frac{a}{X\Delta Y}\right)_{el} = \left(\frac{a}{(X \setminus Y) \cup (Y \setminus X)}\right)_{el} = \left(\frac{a}{X \setminus Y}\right)_{el} \left(\frac{a}{Y \setminus X}\right)_{el}.$$

By the same argument the above is equal to

$$\left(\frac{a}{X}\right)_{el} \left(\frac{a}{Y}\right)_{el} \left(\frac{a}{X \cap Y}\right)_{el}^{-2} = \left(\frac{a}{X}\right)_{el} \left(\frac{a}{Y}\right)_{el}.$$

\square

As an immediate consequence we can use symmetric differences to calculate $\left(\frac{a}{G}\right)_{el}$ in terms of some cyclic subgroups of G :

Corollary 4.9. *If $G = \Delta_{i=1}^t \langle g_i \rangle$, then $\left(\frac{a}{G}\right)_{el} = \prod_{i=1}^t \left(\frac{a}{\langle g_i \rangle}\right)_{el}$.*

Furthermore we obtain:

Corollary 4.10. *For every group G there exists an integer d_G^* such that*

$$\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G^*}{a}\right)$$

for all a satisfying $(a, |G|) = 1$.

Proof. By the previous lemmas we can write G as $\Delta_{i=1}^t \langle g_i \rangle$ and therefore $\left(\frac{a}{G}\right)_{el} = \prod_{i=1}^t \left(\frac{a}{\langle g_i \rangle}\right)_{el}$. By Proposition 3.1 it follows that

$$\left(\frac{a}{G}\right)_{el} = \prod_{i=1}^t \left(\frac{d_{\langle g_i \rangle}}{a}\right)_{el} = \left(\frac{\prod_{i=1}^t d_{\langle g_i \rangle}}{a}\right)$$

so the corollary is proved. \square

Proposition 4.11. *Assume that $G = H \times K$ where H is a nontrivial finite 2-group and K is a finite group of odd order. Then, $\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G}{a}\right)$ for all $(a, |G|) = 1$.*

Proof. Let us write $H = \Delta_{i=1}^h \langle h_i \rangle$ and $K = \Delta_{j=1}^k \langle k_j \rangle$. By Lemma 4.4 we can write $H = \Delta_{i=1}^h \langle h_i \rangle$ with none of the h_i equal to identity. Then, by our previous lemmas, we have $\left(\frac{a}{G}\right)_{el} = \prod_{i=1..h, j=1..k} \left(\frac{a}{\langle(h_i, k_j)\rangle}\right)_{el}$. Since h_i and k_j have relatively prime orders, the cyclic group $\langle(h_i, k_j)\rangle$ has order $o(h_i)o(k_j)$. By Proposition 3.1 we then have that

$$\left(\frac{a}{\langle(h_i, k_j)\rangle}\right)_{el} = \left(\frac{(-1)^{\frac{o(h_i)o(k_j)-2}{2}}}{a}\right).$$

It follows from Corollary 4.9 that

$$\left(\frac{a}{G}\right)_{el} = \prod_{i=1}^h \prod_{j=1}^k \left(\frac{(-1)^{\frac{o(h_i)o(k_j)-2}{2}}}{a}\right) = \prod_{i=1}^h \left(\frac{\prod_{j=1}^k (-1)^{\frac{o(h_i)o(k_j)-2}{2}}}{a}\right).$$

Since k is odd, all of the $o(k_j)$ are odd and all of the $o(h_i)$ are even, so we have that

$$\prod_{j=1}^k (-1)^{\frac{o(h_i)o(k_j)-2}{2}} = (-1)^{\frac{o(h_i)-2}{2}}.$$

Therefore,

$$\left(\frac{a}{G}\right)_{el} = \prod_{i=1}^h \left(\frac{(-1)^{\frac{o(h_i)-2}{2}}}{a}\right) = \left(\frac{a}{H}\right)_{el}.$$

On the other hand, H is a nontrivial 2-group therefore, by Proposition 3.4

$$\left(\frac{a}{H}\right)_{el} = \left(\frac{d_H}{a}\right) = \left(\frac{(-1)^{\frac{|H|-|f_2(H)|}{2}}}{a}\right) = \left(\frac{(-1)^{\frac{|K||H|-|f_2(H)|}{2}}}{a}\right),$$

since K has odd order. Furthermore, since $G = H \times K$ hence $|f_2(G)| = |f_2(H)| > 1$ and $|K||H| = |G|$, thus

$$\left(\frac{a}{H}\right)_{el} = \left(\frac{(-1)^{\frac{|G|-|f_2(G)|}{2}} |G|^{|f_2(G)|}}{a}\right) = \left(\frac{d_G}{a}\right).$$

In other words $\left(\frac{a}{G}\right)_{el} = \left(\frac{d_G}{a}\right)$. □

Theorem 1.5 now follows by Proposition 4.11 and Corollary 3.2.

5. FURTHER REMARKS

Let n be a positive integer. Notice that by identifying $(\mathbb{Z}/n\mathbb{Z})^*$ with the Galois group $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ any non-trivial homomorphism from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\{\pm 1\}$ corresponds an isomorphism

$$\text{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \rightarrow \{\pm 1\},$$

where $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)$ is a quadratic subextension. Therefore, by Chebotarev's density theorem (see [Ma]), any homomorphism from $(\mathbb{Z}/n\mathbb{Z})^*$ to $\{\pm 1\}$ is of the form $\left(\frac{d}{\cdot}\right)$ for some integer d . In particular to any finite group G , by considering the homomorphisms,

$$\left(\frac{\cdot}{G}\right)_{DH} : (\mathbb{Z}/|G|\mathbb{Z})^* \rightarrow \pm 1 \quad \text{and} \quad \left(\frac{\cdot}{G}\right)_{el} : (\mathbb{Z}/|G|\mathbb{Z})^* \rightarrow \pm 1,$$

we can associate a pair number fields K_G and L_G of degree at most two. In this context the main result of Duke and Hopkins is the following: Let Δ_G be the determinant of the character table of G . Then,

$$K_G = \mathbb{Q}(\Delta_G) = \mathbb{Q}(\sqrt{D_G}).$$

It follows that up to square factors D_G is the discriminant of K_G , and hence the name discriminant of G . Notice that by Corollary 4.10 we have that

$$L_G = \mathbb{Q}(\sqrt{d_G^*}).$$

However, it seems that in practice the integer d_G^* is not so easy to calculate. On the other hand for a big class of finite groups, namely the ones described in the hypothesis of Theorem 1.5, we have that

$$L_G = \mathbb{Q}(\sqrt{d_G})$$

and as we observed in Remark 1.3 the integer d_G is quite simple to calculate. We wonder if it is possible to give a simpler description of the field L_G that works for every G .

ACKNOWLEDGEMENTS

In the first place we would like to thank the referee for the various constructive and quite valuable comments and suggestions on the paper. We also thank David Dynerman, Evan Dummit and Jordan Ellenberg for helpful comments on an earlier version of this paper, and the organizers of the group theory seminar at UW-Madison for allowing us to present the results of this paper, and for their helpful feedback.

REFERENCES

- [D-H] Duke. William, Hopkins. Kimberly, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly **112** (2005), no. 3, 251-256.
- [I-R] Isaacs. I.M, Robinson. G.R, *On a theorem of Frobenius: Solutions to $x^n = 1$ on finite groups*, Amer. Math. Monthly **99** (1992), no. 4, 352-354.
- [Ma] D. Marcus, *Number Fields*, Universitext. Springer-Verlag, New York-Heidelberg, 1977. viii+279 pp.
- [Z] Zolotarev. G, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouvelles Ann. Math. (2) **11** (1872) 354-362.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, 480 LINCOLN DRIVE,
MADISON, WI 53705 USA
E-mail address: hablics@math.wisc.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD,
VANCOUVER, BC V6T 1Z2 CANADA
E-mail address: mantilla@math.ubc.ca